BAB III

METODOLOGI PENELITIAN

3.1 Objek Penelitian

Dengan dilakukannya penelitian ini, peneliti bertujuan untuk melakukan pengukuran terhadap perilaku keamanan melalui kebiasaan pengguna smartphone Android, maka dari itu diperlukannya respon dari pengguna smartphone Android dalam melakukan pengamanan dan mengukur dari hasil respon dalam mencegah dan mengamankan informasi atau data penting yang tersimpan.

Penelitian dilakukan dengan penyebaran kuisioner terhadap calon responden secara *snowball* dengan rentang umur 39-51 tahun. Penyebaran kuisioner hanya berfokus kepada daerah Jabodetabek.

3.2 Populasi dan Sample

Populasi bukan sekedar jumlah yang ada pada objek/subjek yang dipelajari, tetapi meliputi seluruh karakteristik atau sifat yang dimiliki oleh subjek atau objek itu. (Sugiono, 2011). Sampel adalah suatu bagian dari populasi tertentu yang menjadi perhatian (Suharyadi dan Purwanto, 2004).

Menurut Hair et al (Kiswati, 2010) sampel yang *representative* adalah tergantung pada jumlah indikator dikali 5 (lima) sampai 10 (sepuluh). Menurut hair et al (Prawira, 2010) merekomendasikan jumlah sampel minimal adalah 5-10 kali dari jumlah item pertanyaan yang terdapat di kuesioner.

Penelitian memiliki 31 pertanyaan dengan 6 indikator variabel, maka sebagai berikut:

Minimum sampel = 31 x 6 = 186 responden

Berdasarkan perhitungan di atas maka didapatkan minimum sampel sebanyak 186 responden.

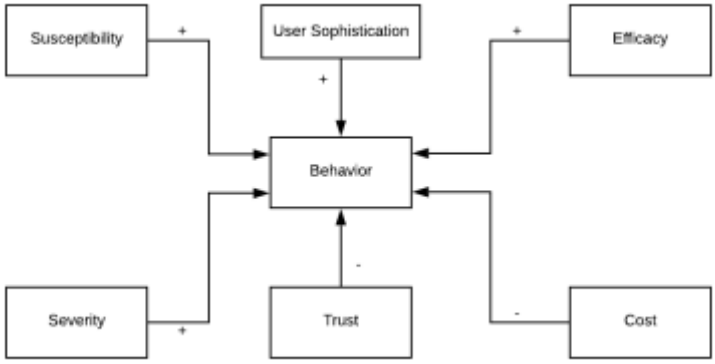
3.3 Metode Penelitian

Metode penelitian akan menggunakan *Partial Least Square* yang bertujuan untuk mengukur perilaku keamanan pengguna smartphone Android. Berbagai ancaman keamanan terhadap telepon pintar (FCC: Komisi Komunikasi Federal, 2012; Ofcom, 2013; ENISA: Badan Uni Eropa untuk Keamanan Jaringan dan Informasi, 2010) dapat dikelompokkan ke dalam setidaknya tiga kategori (He, 2013):

(1) Malware, seperti worm dan virus, bertujuan merusak perangkat atau menjadikannya tidak tersedia. Malware dapat menghapus file-file penting, menguras baterai atau mengganggu kemampuan komunikasi smartphone.

(2) Kebocoran data, yaitu pengumpulan dan transmisi data yang tidak sah seperti lokasi, kontak, dan perilaku penggunaan. Banyak aplikasi pihak ketiga (dan penyedia sistem yang beroperasi, berpotensi) mengumpulkan pengguna secara diam-diam, tanpa atau di luar persetujuan pengguna, mengirimkan kembali data ini ke pengembang untuk tujuan penambangan data atau pemasaran, sehingga melanggar privasi pengguna.

(3) pencurian informasi rahasia yang disengaja, seperti kata sandi dan data kartu kredit. Serangan peretasan yang ditargetkan untuk mencegat dan mendekripsi komunikasi, pemasangan Trojan dan spyware, serta serangan phishing dengan spoofing atau peniruan, dapat digunakan untuk mencuri informasi rahasia untuk spionase, pemerasan atau tebusan.



Gambar 3. 1 Expectacy Based Model

Sumber : (Das and Khan, 2015)

Dengan demikian, kerentanan dioperasionalkan dengan tiga pertanyaan tentang kerentanan terhadap masalah keamanan: satu untuk malware, satu lagi untuk kebocoran data dan yang ketiga untuk pencurian data. Hal yang sama berlaku untuk tingkat keparahan: terdiri dari masing-masing item untuk potensi kerusakan yang dirasakan dari malware, kebocoran data, dan pencurian data.

Selain efek langsung kerentanan dan keparahan pada perilaku keamanan, kami juga mengakui ke dalam model kami istilah interaksi multiplikasi yang dibentuk oleh dua variabel independen ini. Penyesuaian statistik yang diperlukan untuk mengakomodasi istilah interaksi ini dibahas di bagian analisis data.

Tiga item untuk kemanjuran respons merujuk pada efektivitas tindakan keamanan yang dirasakan terhadap malware, pencurian data, dan kebocoran data. Biaya juga termasuk item keempat selain hilangnya kenyamanan, fungsionalitas, dan waktu dalam melindungi dari malware, kebocoran data, dan pencurian. Elemen biaya ini mengacu pada biaya sosial karena tidak menggunakan fitur atau aplikasi ponsel cerdas yang populer di antara teman-teman seseorang: kemungkinan dikecualikan dari percakapan, diskusi, dan aktivitas yang dilakukan melalui media sosial.

Karena target penelitian kami menyadari perilaku daripada sikap, kami memilih ukuran kecanggihan pengguna yang ditunjukkan alih-alih kemanjuran yang dirasakan. Kecanggihan pengguna adalah untuk mempelajari perilaku keamanan kami apa self-efficacy untuk studi niat: ukuran kemampuan pengguna untuk mempertahankan diri terhadap keamanan ancaman. Dalam studi ini, kami menggunakan jumlah aplikasi yang diinstal pada ponsel cerdas pengguna sebagai proxy untuk kecanggihan pengguna. Kami berharap "pengguna yang kuat" menginstal lebih banyak aplikasi daripada lebih banyak pengguna pemula (Das and Khan, 2016).

Dalam menggunakan teknologi sosial, pengguna smartphone mungkin dipengaruhi oleh tingkat kepercayaan mereka secara keseluruhan pada pengguna lain. Kepercayaan, dalam hal ini, adalah pusat keamanan informasi (yang bertujuan untuk membangun dan mempertahankan kepercayaan), dan ada panggilan untuk membuat peran kepercayaan tersebut eksplisit (Jensen, 2012) dan tidak ambigu (Gollmann, 2006). Kami menggunakan tiga item ukuran kepercayaan yang

diperoleh dari Survei Umum Sosial Amerika (GSS), 2014 dan kuesioner Panel Sosial-Ekonomi Jerman (SOEP: Panel Sosial-Ekonomi, 2014).

Pengguna smartphone yang lebih percaya mungkin diharapkan untuk menampilkan perilaku keamanan tingkat rendah, karena mereka cenderung tidak mengharapkan tindakan jahat dari orang lain.

Respons terhadap ancaman keamanan telah dilihat secara universal sebagai keputusan biaya-manfaat: mengadopsi tindakan balasan jika biaya melakukannya kurang dari kerugian yang diharapkan dari ancaman yang dilindunginya. Oleh karena itu, kami menghubungkan perilaku keamanan secara langsung dengan manfaat biaya yang dirasakan pengguna dari merespons ketiga ancaman - malware, kebocoran data dan pencurian data. Karena itu, hanya diperlukan item kuesioner yang sama untuk dikelompokkan secara berbeda - kali ini sesuai dengan garis ancaman. Untuk selanjutnya, kami menyebut model alternatif ini sebagai model perilaku keamanan smartphone "berbasis ancaman".

Untuk setiap ancaman, kami mendefinisikan manfaat biaya dari menanggapi ancaman sebagai jumlah kerentanan dan tingkat keparahannya, ditambah kemanjuran respons keamanan, dikurangi biaya perlindungan terhadapnya. Ini mencerminkan intuisi kami bahwa perilaku keamanan lebih mungkin dilakukan untuk ancaman kerentanan tinggi dan keparahan, dan ketika kemanjuran responsnya dianggap tinggi. Biaya melakukan perilaku keamanan (dalam fungsi, kenyamanan atau waktu) mengurangi daya tarik perilaku keamanan dan membuatnya lebih kecil kemungkinannya untuk dilakukan.

Metode Partial Least Square memiliki beberapa tahapan dalam menguji validitas dan realibilitas, yaitu (SmartPLS, 2016) :

1. Outer Model

Terdapat dua tahap pengujian pada outer model, yaitu sebagai berikut (Sugiyono, 2017):

A. Uji Validitas

Terdua dua tahap pengujian untuk menentukan validitas, yaitu sebagai berikut (Sugiyono, 2017; Haryono, 2017):

i. Convergent Validity

Pada validitas konvergen dikatakan ada jika *standardized path loading coefficient* untuk panah struktural dari faktor formatif InsentifF ke faktor reflektif InsentifR tinggi (Garson, 2016) . (Chin, 1998) menyarankan potongan 0,90 atau setidaknya 0,80. Ini menyiratkan bahwa nilai R-squared untuk faktor reflektif harus 0,81 atau setidaknya 0,64.

Average variance extracted (AVE) dapat digunakan sebagai uji validitas konvergen dan divergen. AVE mencerminkan komunitas rata-rata untuk setiap faktor laten dalam model reflektif (Garson, 2016). Dalam model yang memadai, AVE harus lebih besar dari 0,5 (Chin, 1998; Höck & Ringle, 2006: 15) serta lebih besar dari cross-loadings,

yang berarti faktor harus menjelaskan setidaknya setengah dari varian masing-masing indikator. AVE di bawah .50 berarti varians kesalahan melebihi varians yang dijelaskan.

ii. Discriminant Validity

Pada *discriminant validity*, ada beberapa hal yang harus di perhatikan untuk melakukan pengujian validitas. Yang pertama, akar kuadrat dari AVE harus lebih tinggi dari korelasinya dengan variabel laten lainnya (Fornel dan Larcker, 1981).

Yang kedua, *cross-loadings* adalah alternatif untuk AVE sebagai metode penilaian validitas diskriminan untuk model reflektif. Paling tidak, tidak ada variabel indikator yang memiliki korelasi lebih tinggi dengan variabel laten lain daripada dengan variabel latennya sendiri. Jika ya, model tidak ditentukan secara tepat (Garson, 2016).

B. Uji Reabilitas

Pada pengujian reabilitas, terdapat dua tahap yang perlu diperhatikan, yaitu sebagai berikut (Sugiyono, 2017; Haryono, 2017):

i. Cronbach’s Alpha

Pada cronbach's alpha jika data lebih besar atau sama dengan 0,80 untuk skala yang baik, 0,70 untuk skala yang dapat diterima, dan 0,60 untuk skala untuk tujuan eksplorasi (Garson, 2016).

ii. Composite Reability

Composite reability adalah alternatif pilihan untuk cronbach's alpha sebagai tes *convergent validity* dalam model reflektif. *Composite reability* dapat menyebabkan estimasi keandalan yang sebenarnya lebih tinggi. Batas yang dapat diterima untuk *composite reability* sama dengan untuk ukuran keandalan apa pun, termasuk alpha cronbach. *Composite reability* bervariasi dari 0 hingga 1, dengan 1 keandalan estimasi sempurna. Dalam model yang memadai untuk tujuan eksplorasi, composite reability ≥ 0,6 (Chin, 1998; Höck & Ringle, 2006); ≥ 0,70 untuk model yang memadai untuk tujuan konfirmasi (Henseler, Ringle, & Sarstedt, 2012); dan ≥ 0,80 dianggap baik untuk penelitian konfirmasi (Daskalakis & Mantas, 2008).

2. Inner Model

Terdapat dua tahap pengujian inner model, yaitu sebagai berikut (Sugiyono, 2017; Haryono, 2017):

A. Uji R-*Square*

R-square, juga disebut koefisien determinasi. (Hock dan Ringle, 2006) menjelaskan hasil di atas batas 0,67, 0,33 dan 0,19 masing-masing menjadi "substansial", "sedang" dan "lemah".

B. Uji Signifikasi

Setelah menjalankan opsi bootstrapping, nilai di dalam path diagram adalah nilai untuk uji t- signifikansi. Semua t-*values* ≥ 1,96 signifikan pada tingkat 0,05, yang merupakan kasus untuk semua t-*values* juga dapat diatur ke "P *values*" untuk mendapatkan tingkat probabilitas (Garson, 2016).

PLS-Multi Group Analysis (MGA): Tes signifikansi non-parametrik ini menemukan perbedaan menjadi signifikan jika nilai p ≤ 0,05 untuk perbedaan kelompok-spesifik *path coefficient*s (Sarstedt et al., 2011) merupakan tes yang paling umum digunakan.

3.4 Alat Penelitian

Tabel 3. 1 Perbandingan Alat Penelitian

PARAMETER PEMBANDING	LISREL & AMOS	SMART PLS
Asumsi distribusi	Distribusi harus memenuhi syarat normalitas.	Tidak mengharuskan data terdistribusi normal.
Error Software	Bermasalah terhadap *inadmissibile* dan *factor indeterminancy.*	Tidak menghadapi masalah dalam menjalankan iterasi model.
Pengujian signifikansi	Model dapat diuji dan difalsifikasi dengan estimasi parameter dan uji kelayakan model (GOF).	Tidak dapat diuji dan difalsifikasi meskipun estimasi parameter dapat dilakukan, uji kelayakan model tidak dapat dilakukan.

PARAMETER PEMBANDING	LISREL & AMOS	SMART PLS
Basis teori	Harus mempunyai dasar teori yang kuat	Pengujian model dapat dilakukan tanpa dasar teori yang kuat
Sifat konstruk	Reflektif.	Reflektif dan formatif.

Tabel 3.1 menunjukkan perbandingan alat penelitian antara LISREL & AMOS, dan AMOS. Penelitian menggunakan *tools* Smart PLS dikarenakan tools tersebut model dapat diuji sesuai dengan metode penelitian.(Abdillah & Jogiyanto, 2015). Smart PLS merupakan sebuah *tools* yang berfungsi untuk menganalisa *partial least square*s. Smart PLS juga memiliki UI dan UX yang *user-friendly* dan gratis untuk *license* tertentu (Garson, 2016).

Smart PLS memiliki *graphical user interface* yang memungkinkan pengguna untuk mengestimasi PLS *path model*. Hingga saat ini, Smart PLS merupakan salah satu program yang paling mudah untuk dimengerti dan paling maju di lapangan (Hair, Hult, Ringle, & Sarstedt, 2017).

3.5 Teknik Pengumpulan Data

Penelitian menggunakan metode kuesioner yang disebar secara *snowball* menggunakan google form dengan jumlah responden sebanyak 155 orang yang rentang umur 39-51 tahun di jabodetabek.

Pengumpulan data menggunakan skala likert sebagai indikator pengukuran dimana sebagai berikut :

1 = Sangat Tidak Setuju	Diberikan skor 1
2 = Tidak Setuju	Diberikan skor 2

3 = Netral	Diberikan skor 3
4 = Setuju	Diberikan skor 4
5 = Sangat Setuju	Diberikan skor 5

Pertanyaan pada penilitian dibentuk sesuai dengan penelitian sebelumnya, dimana kuisioner terdari dari 30 pertanyaan yang menjadi indikator mewakilkan ke-lima variabel independent dan satu variable dependen, dimana pertanyaan yang dibuat sebagai berikut :

Tabel 3. 2 Pertanyaan Partial Least Square

	User Sophistication
P1	Jumlah aplikasi yang Anda gunakan
	Behavior
P2	Saya mengunci smartphone Android saya dengan sidik jari / kata sandi / pin / pola
P3	Saya mengupdate aplikasi secara berkala
P4	Saya menginstall antivirus di smartphone Android
P5	Saya melakukan enkripsi pada data-data sensitif saya
P6	Saya tidak menyimpan data-data rahasia di smartphone
P7	Saya melihat Review / Rating dari aplikasi sebelum menginstal sebuah aplikasi
	Susceptibility
P8	Beberapa Aplikasi / Website yang saya gunakan mengandung Virus dan menginfeksi smartphone saya
P9	Beberapa aplikasi/ Website yang saya kunjungi mengandung MALWARE dan dapat menginfeksi smartphone saya
P10	Aplikasi smartphone bisa saja mengirim data pribadi (Seperti Lokasi saya, kontak saya, dll) tanpa sepengetahuan saya

P11	Informasi sensitif saya dapat dicuri ketik saya mengakses Aplikasi/Web/Email dari semua jenis smartphone
	Severity
P12	VIRUS dapat mengakibatkan fungsi smartphone saya tidak berjalan dengan semestinya
P13	MALWARE dapat mengakibatkan fungsi smartphone saya tidak berjalan dengan semestinya
P14	Kebocoran informasi sensitif dapat mengakibatkan saya mengalami kerugian secara materi (password, data bank, dll)
P15	Pencurian data dapat mengakibatkan masalah yang cukup sulit
	Efficacy
P16	Saya dapat menghentikan VIRUS dengan cara menghindari sumber " Aplikasi / Website yang tidak di kenal "
P17	Saya dapat menghentikan MALWARE dengan cara menghindari sumber " Aplikasi / Website tidak di kenal "
P18	Saya dapat menghentikan VIRUS dengan cara menghindari sumber " Aplikasi / Website "mencurigakan"
P19	Saya dapat menghentikan MALWARE dengan cara menghindari sumber " Aplikasi / Website "mencurigakan"
P20	Saya dapat menentukan akses terhadap data personal saya (Seperti Kontak, Lokasi, dll) dengan mereview fitur keamanan aplikasi sebelum di install pada smartphone saya
P21	Saya dapat melindungi data-data sensitif saya dengan melakukan enkripsi di smartphone saya
	Cost
P22	Menghindari rasa ingin tahu terhadap Aplikasi / Website karena takut akan VIRUS membuat saya menjadi kurang nyaman
P23	Menghindari rasa ingin tahu terhadap Aplikasi / Website karena takut akan MALWARE membuat saya menjadi kurang nyaman
P24	Saya tidak memiliki waktu untuk melakukan review keamanan pada aplikasi sebelum di install dan di gunakan
P25	Saya merasa kurang nyaman dengan mengekripsikan data-data saya

P26	Saya menggunakan aplikasi yang dipakai Keluarga/Teman
	Trust
P27	Pada umumnya saya berbicara mengenai informasi sensitif saya kepada orang yang saya percaya
P28	Saya sangat berhati-hati dalam membuat kesepakatan dengan orang lain
P29	Saya berpikir orang lain dapat mengambil keuntungan dari saya apabila diberikan kesempatan
P30	Orang lain bersikap adil terhadap saya
P31	Saya perlu mempercayai orang sebelum melakukan kesepakatan dengan orang yang tidak di kenal

Pertanyaan-pertanyaan tersebut dibentuk berdasarkan keberhasilan dalam menanggapi ancaman yang terjadi, sehingga dapat diasumsikan pertanyaan-pertanyaan tersebut mewakili pengetahuan pengguna terhadap ancaman yang ada, apakah pengguna telah memahami ancaman, resiko serta biaya yang mereka dapat rasakan (Das and Khan, 2016).

3.5 Teknik Analisis Data

Data yang telah disebarkan dan dikumpulkan kepada semua responden, akan diolah dan diukur agar nantinya dapat ditentukan apakah terdapat keterkaitan antara perilaku pengguna terhadap keamanan pengguna, teknik analisis data yang akan digunakan adalah *Multiple Regression* (Regresi linier berganda).

Penelitian ini menggunakan *Multiple regression* (regresi linier berganda) dimana variabel bebas yang digunakan lebih dari satu sehingga apabila menggunakan *Linear regression* (regresi linier) tidak terlalu cocok untuk digunakan, karena tidak dapat mengukur secara keseluruhan variabel bebas lebih dari satu sedangkan pada metode *multiple regression* (regresi linier berganda)

variabel bebas lebih dari satu sangat memungkinkan untuk dianalisis. Setelah ditemukan hasil dari perhitungan *multiple regression* maka hasilnya tersebut akan diuji sesuai dengan hipotesa yang telah di tentukan.

Tool yang digunakan adalah Smart PLS, terdapat juga tools pengolahan data yang lain yaitu Microsoft Excel. Namun lebih baik menggunakan Smart PLS dibandingkan Microsoft Excel dikarenakan keterbatasan fungsi yang tersedia.

3.6 Variabel Penelitian

Dari *Partial Least Square* dapat ditentukan variable dependen dan independent yang akan digunakan, yaitu :

Tabel 3. 3 Variabel Dependen dan Independen

Dependen Variabel	Independen Variabel
Behavior	User Sophistication Susceptibility Severity Efficacy Cost Trust

3.7 Hipotesis

Hipotesis yang akan disusun dalam penelitian adalah hipotesis H1 dimana terjadinya pengaruh (penerimaan) antara variabel independen terhadap variabel dependen untuk masing-masing model dengan signifikasi sebesar 5%, berikut dapat dijelaskan variabel masing-masing dari tiap model, sebagai berikut :

1. *User Sophistication*

User Sophistication atau disebut juga kecanggihan pengguna, merupakan salah satu variabel yang akan diukur, menurut penelitian terdahulu, *user sophistication* yang semakin tinggi di harapkan akan membuat pengguna jauh lebih mengerti dalam pemanfaatan teknologi, sehingga semakin tinggi *user sophistication* maka di harapkan *behavior* pengguna akan semakin baik (Das and Khan, 2015), maka dari itu hipotesis yang akan diajukan mengenai *user shopiscation* sebagai berikut :

H1 = *User sophistication* berpengaruh signifikasi positif terhadap *behavior*.

2. *Susceptibility*

Susceptibility atau disebut juga kerentanan adalah salah satu variabel yang akan diukur, *susceptibility* dibentuk berdasarkan ancaman-ancaman yang dapat menjadi dampak bagi para pengguna, sebagian besar penelitian sebelumnya mengenai perilaku keamanan secara implisit atau eksplisit mengangkat *expectacy framework* dimana *susceptibility* yang dirasakan dan *efficacy* yang dirasakan bergabung mendorong proses penilaian ancaman yang melengkapi penilaian dari menanggulangi tanggapan berdasarkan analisis *cost-benefit* dari tindakan pengamanan dan seberapa besar kemungkinannya langkah-langkah tersebut untuk berhasil menetralisir ancaman. Ini menjadi sama dengan sejumlah kerangka kerja bisnis yang digunakan untuk manajemen risiko keamanan informasi yang juga melihat perilaku keamanan sebagai *tradeoff* antara risiko - dioperasionalkan sebagai kerugian tahunan harapan dan biaya

(Fenz et al., 2014), dengan memahami ancaman-ancaman yang dapat menyebabkan masalah bagi para pengguna, maka di harapkan *behavior* pengguna akan semakin baik (Das and Khan, 2015), maka dari itu hipotesis untuk variabel *susceptibility* dapat dibentuk sebagai berikut :

H1 = *Susceptibility* berpengaruh signifikasi positif terhadap *behavior*

3. *Severity*

Penelitian terdahulu menunjukkan bahwa *susceptibility* yang dirasakan, *severity* yang dirasakan, *efficacy* dan respon *cost* mempengaruhi niat perilaku untuk menggunakan perangkat lunak *anti-spyware* sebagai teknologi pelindung (Chenoweth et al, 2009). Penelitian selanjutnya yang menemukan bahwa *severity* Adanya pengaruh ini dari penelitian terdahulu membuat variabel *severity* dapat dibentuk menjadi sebuah hipotesa sebagai berikut :

H1 = *Severity* berpengaruh signifikasi positif terhadap *behavior*

4. *Efficacy*

Penelitian tentang niat pengguna untuk menggunakan *anti-spyware*, menemukan bahwa niat tersebut dipengaruhi secara langsung oleh respon yang keberhasilan, *self-efficacy* dan norma sosial, namun tidak dengan kerentanan dan tingkat keparahan ancaman seperti yang digambarkan dalam ketakutan banding (Johnston dan Warkentin, 2010). Penelitian lain

menemukan pemenuhan niat bergantung pada persepsi *efficacy* keamanan dan juga tanggapan pengguna *self- efficacy* dalam hal melakukan tanggapan (Ifinedo, 2012). Berdasarkan penelitian-penelitian terdahulu maka variable efficacy dapat membentuk sebuah hipotesis sebagai berikut :

H1 = *Efficacy* berpengaruh signifikasi positif terhadap *behavior*

5. *Cost*

Penelitian terdahulu mengembangkan dan menguji model penghindaran ancaman teknologi menemukan bahwa motivasi untuk menghindari *spyware* dipengaruhi secara positif oleh ancaman yang dirasakan (*susceptibility* dan *severity*), *self-efficacy* dan secara negatif terhadap *cost* (Liang dan Xue, 2010). Variabel *cost* dapat di bentuk hipotesis sebagai berikut :

H1 = *Cost* berpengaruh signifikasi negatif terhadap *behavior*

6. *Trust*

Penelitian terdahulu yang menggunakan variabel *trust* menemukan bahwa kualitas informasi kebijakan keamanan memiliki dampak positif terhadap niat dan penyesuaian perilaku, terlepas dari sikap kebijakan pengguna, kepercayaan dan kebiasaan (Pahnila et al, 2007), berdasarkan penelitian diatas dapat dibentuk sebuah hipotesis sebagai berikut :

H1 = *Trust* berpengaruh signifikasi negatif terhadap *behavior*

Penjelasan-penjelasan dari masing-masing variabel diatas maka akan disusun kedalam masing-masing model, pada model *Partial Least Square* kesimpulan hipotesis yang dibentuk sebagai berikut:

Tabel 3. 4 Hipotesis Partial Least Square

	Deskripsi
H1	*User Sophistication* berpengaruh signifikasi positif terhadap *behavior*
H2	*Susceptibility* berpengaruh signifikasi positif terhadap *behavior*
H3	*Severity* berpengaruh signifikasi positif terhadap *behavior*
H4	*Efficacy* berpengaruh signifikasi positif terhadap *behavior*
H5	*Cost* berpengaruh signifikasi negatif terhadap *behavior*
H6	Trust berpengaruh signifikasi negatif terhadap behavior